Federal Trade Commission

Remarks of Chairman Deborah Platt Majoras[1]

The Exchequer Club
Washington, D.C.
September 20, 2006

I. Introduction

I am pleased to be here this afternoon to speak to the Exchequer Club of Washington, D.C., and I thank Ronald Glancz for inviting me. Even after two years at the helm of the Federal Trade Commission, I still am amazed at the number of consumer and economic issues that our diverse and vibrant economy produces. As a law enforcement agency of general jurisdiction, the FTC plays a role in issues ranging from competition in gasoline markets to the successful Do Not Call list; from phony dietary supplements to mortgage and debt collection fraud; from pharmaceutical mergers to childhood obesity; from spam to alcohol advertising – just to skim the surface. Our agency is small by Washington standards, with about 1,100 employees, but our size among other things allows us to nimbly shift resources as new issues of importance to U.S. consumers arise.

During the last two years, an issue that has risen to the top of our agenda is the security of personal data. Information is the new currency, and it moves across the globe in milliseconds through high-speed connections. Magnetic and optical media permit the efficient and cost-

[1] The views expressed herein are my own and do not necessarily represent the views of the Federal Trade Commission or of any other Commissioner.

effective storage of gigabytes of data, and technological developments continue to emerge at a dizzying pace. This is good news for the marketplace and good news for consumers. With great innovations, however, typically come risks, and fortunately, we, as a nation, are learning that data security is critical to reaching our full potential in the information economy.

II. Data Security

A. Private Sector Security Challenges

The question is whether we are learning quickly enough. Although many organizations are realizing that strong privacy protections can enhance consumer trust and satisfaction, surveys continue to present troubling data.[2] The Enterprise Strategy Group recently surveyed 227 IT professionals, and 25% of the respondents characterized their organizations as vulnerable or very vulnerable to a breach.[3] The same number rated their organizations as fair or poor in protecting data. A recent survey from the Small Business Technology Institute provides similarly alarming news: over half of all small businesses in the U.S. experienced a breach within the past year; nearly 20% of small businesses do not use virus scanning for email; more than 60% do not

---

[2] Studies have shown that security breaches that compromise confidential consumer data create significant problems for businesses. A 2005 Ponemon Institute survey of more than 1,000 victims of data security breaches found that nearly 20% had terminated their relationship with the company that had maintained their data, and another 40% said they might terminate their relationship. *See* "Data Security Breaches Impact Corporate Bottom Lines." *PR Newswire* (Sept. 26, 2005), *available at* http://www.prnewswire.com.

[3] *See* "Enterprise Strategy Group Report Reveals that Security Professionals Claim that Confidential Data is Most Vulnerable on Laptop Computers," *Business Wire* (Mar. 27, 2006).

protect wireless networks by encrypting; and a full two-thirds do not have an information security plan.[4]

Without question, businesses confront many challenges in making data secure. For example, the use of portable data storage devices – such as thumb drives or flash drives and disk-based MP3 players – is emerging as a serious security concern. These devices allow us to store vast amounts of data on tiny devices that have broad compatibility with most computers; I am betting that many, if not most, of the people in this room have used such devices for presentations and when traveling. Yet, as these devices become smaller and cheaper, with increased storage capacity and faster transfer speeds, the potential risks increase. They are small and easy to misplace, and the amount of data they can hold is astounding. Personal information for hundreds of thousands – or even millions – of people could fit on a typical USB thumb drive.

IT professionals confront such challenges every day. Fortunately, the market is developing solutions. Flash drives now are available with enhanced security features, such as encryption or biometrics that require fingerprint matching before the data can be accessed. Software allows information technology managers to control whether an individual user can connect a portable data storage device, such as an iPod or a USB flash drive, to a company computer. Solutions exist for many of our IT security problems, and more solutions are developed everyday. The key is to use them. All organizations have a collective responsibility to keep personal data secure.

---

[4] *See* Market Survey and Analysis Report, *Small Business Information Security Readiness*, Small Business Technology Institute (July 2005).

B. FTC Law Enforcement Actions

The FTC's goal is to create a culture of security for sensitive information so that businesses and other organizations (including government agencies) prevent potentially harmful data breaches. We need to start treating personal data as we treat cash – because that is what it represents to an identity thief. In recent years, the Commission has nurtured the development of a set of sensible legal principles – with the assistance of industry, consumer groups, and other government agencies, including the banking agencies, with which we work particularly closely. The laws and rules we enforce are intended to establish realistic, workable, and enforceable standards that facilitate rather than inhibit the flow of commerce.

Unfortunately, some have been slow to act. Accordingly, over the past 18 months, the FTC has deployed the agency's full arsenal of statutory tools to bring cases against companies that failed to implement reasonable measures to protect sensitive consumer information. The Commission's enforcement tools derive from Section 5 of the FTC Act,[5] which prohibits unfair or deceptive acts or practices, the Safeguards Rule, and the Fair Credit Reporting Act ("FCRA").[6]

The principle that a company should implement reasonable and appropriate security for sensitive information is codified in the Commission's Gramm-Leach-Bliley Safeguards Rule. The Rule was issued in May 2002 after a two-year rulemaking process in which the FTC received and analyzed comments from stakeholders in the public and private sectors. The Safeguards Rule requires "financial institutions" that fall within the FTC's jurisdiction to

---

[5] 15 U.S.C. § 45.

[6] 15 U.S.C. §§ 1681-1681x.

implement reasonable safeguards for their data,[7] acknowledging that what is "reasonable" depends on the sensitivity of the information, the potential risks to the information, and the costs of avoiding those risks. The Rule is process-oriented – firms must evaluate the risks to their data, establish policies to address those risks, develop a system to implement protections, and review and when necessary amend the policies periodically, because risks evolve over time.

When evaluating the reasonableness of a company's information security program, even outside of the Gramm-Leach-Bliley context, the Safeguards Rule principles are the touchstone. In our investigations, we look at the overall security system that the firm has implemented and its *reasonableness* in light of the size and nature of the business, the nature of the information it maintains, the security tools that are available, and the security risks it faces.

I emphasize that the standard is "reasonableness," not perfection. Thus, the fact that a company suffered a breach does not, in and of itself, establish that its practices were unreasonable, although it could be evidence of that fact. In many investigations, the staff has concluded that, although a breach occurred, the company did have reasonable procedures in place to safeguard the data.

1. Recent Commission Cases

In May, the Commission announced our 13th case involving data security, Nations Title Agency.[8] NTA, a privately-held company that provides real-estate related services through 57 subsidiaries in 20 states, promised consumers that it maintained "physical, electronic and

---

[7] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[8] *Nations Title Agency, Inc.*, File No. 052-3117 (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/nationstitle.htm

procedural safeguards." Although many of our data security cases emphasize high-tech security issues, this case serves as a reminder not only that securing high-tech data is essential, but that we cannot forget the low-tech. Reasonable security practices include both. In this case, we allege that the respondents failed to provide reasonable and appropriate security for consumers' personal information, and that on at least one occasion, a hacker – using a common website attack – was able to obtain access to the subsidiaries' computer network. In addition, we allege that one of NTA's subsidiaries disposed of documents containing personal consumer information by simply tossing the documents into an unsecured dumpster. The complaint states claims for violations of the GLB Safeguards and Privacy Rules and under Section 5 of the FTC Act. Respondents agreed to settle the charges by entering into a Consent Order that requires them to implement a comprehensive security program and obtain a third-party audit showing compliance.[9]

No one need worry that the FTC is looking for "perfect" security, or that we are developing a de facto strict liability standard for when a breach occurs, because the cases we have brought have not been close calls. The ChoicePoint high-profile breach that occurred last year provides another example.[10] In the resulting case, we alleged that consumer data broker,

---

[9] The Commission did not allege violations of the Fair and Accurate Credit Transactions Act (FACTA) Disposal Rule, which requires businesses and individuals to take reasonable and appropriate measures to dispose of sensitive information derived from consumer reports, because the dumpster incident occurred prior to the effective date of that Rule. But going forward, I think you can safely assume that tossing personal consumer report information into an unsecured dumpster runs afoul of the Disposal Rule.

[10] The FTC issued a four count complaint against ChoicePoint: Counts I and II alleged violations of the FCRA, Count III alleged that ChoicePoint engaged in unfair practices in violation of Section 5 of the FTC Act, and Count IV alleged that ChoicePoint engaged in deceptive acts or practices in violation of Section 5 of the FTC Act. *United States v.*

ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and that these failures allowed data thieves to obtain access to the personal information of more than 160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. The Commission obtained $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in an FTC case – $5 million in consumer redress for identity theft victims, and significant injunctive provisions that require ChoicePoint to implement a variety of new data security measures.

C. Government Breaches

Keeping consumers' data secure is essential for the public sector as well. I am well aware that the numerous reports of data breaches within the federal government over the past few months have shaken our citizens' trust in our data security. The incident with the highest profile, of course, was the theft of a Veterans Administration laptop and external hard drive that contained personally identifiable information for about 17.5 million veterans and active duty military personnel.[11] (Fortunately, the VA incident was resolved on a reassuring note: the laptop and hard drive were recovered, and the FBI's forensic examination of the equipment concluded

---

ChoicePoint, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf.

[11] The Department of Veterans Affairs initially reported that as many as 26.5 million people could have been affected by the data breach, but it was subsequently discovered that some of the data was duplicative or did not contain Social Security numbers. *See* Goldfarb, Zachary A. "VA to Offer Credit Monitoring," *The Washington Post*, June 22, 2006 at A27.

that the sensitive files were neither accessed nor compromised.[12]) But that was not the only breach,[13] and we acknowledge that your government also has work to do.

These breaches inspired swift and strong responses. For example, in August, the V.A. announced that all of its computers would be updated with enhanced data security encryption systems. And at the FTC, I assembled a team that took immediate action, reviewing the different types of sensitive data that the agency collects, and updating our procedures and policies regarding maintaining and protecting the data. And going forward, we will continue to review and monitor how we handle and secure the sensitive data that is essential for us to fulfill our missions.

III. Identity Theft

For consumers, trust in an economic medium is critical, whether it be on-line shopping or banking or just the use of credit and debit cards. Aside from general privacy concerns, consumers whose personal data has been stolen or improperly released are concerned about identity theft, a particularly pernicious crime that requires swift action on many fronts. Like a virus, it spreads through our economic system, striking randomly and often inflicting great harm on innocent victims. According to a San Jose, California consumer who called the FTC's consumer help line, in just one day identity thieves opened nine credit card accounts in her name

---

[12] *See* Lee, C. and Goldfarb, Z. "Stolen VA Laptop and Hard Drive Recovered." *The Washington Post*, June 30, 2006 at A01.

[13] I regret that even the FTC experienced a data security breach when a laptop containing some personal information on 110 individuals, some of whom were FTC defendants, was stolen from a locked vehicle.

and incurred $15,000 in charges. Unfortunately, this victim's tale is not unusual – and it is far from the most egregious case. We cannot allow consumers' trust to be further eroded.

The 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act") assigned the FTC a unique role in combating identity theft and coordinating government efforts.[14] While we cannot prosecute the crime because we have only civil jurisdiction, we take consumer complaints and implement the Identity Theft Data Clearinghouse, a centralized database of victim complaints used by 1,300 law enforcement agencies; assist victims and consumers who wish not to be victims by providing information and education; and educate businesses on sound security practices.

A. Identity Theft Task Force

On May 10, 2006, the President issued an Executive Order that created the Identity Theft Task Force,[15] appointing Attorney General Gonzalez the Chairman of the Task Force and me as Co-Chairman. Ronald Tenpas, an Associate Deputy Attorney General at DOJ, is the Executive Director of the Task Force, and FTC Bureau of Consumer Protection Director Lydia Parnes serves as Deputy Director. By creating this Task Force – which includes representatives from more than a dozen federal agencies – the President has underscored the importance of the government's role in the fight against identity theft and the need to prevent, investigate, and prosecute identity theft crimes and deliver just and effective punishment to those who perpetrate them.

---

[14] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

[15] *See* Exec. Order No. 13,402, 71 F.R. 27,945 (2006)

The Task Force has three primary goals: (1) to increase aggressive law enforcement actions, (2) to improve outreach to better educate our citizens on what they can do to avoid being victimized and our businesses on how they can implement better security measures to protect personal data, and (3) to increase federal agency safeguards to better protect secure, government-held data. The Task Force is working to create a coordinated, national response to identity theft, and we will present a strategic plan to the President this November.

Yesterday, the Task Force announced a series of interim recommendations that could be implemented quickly and that we thought should not wait until the final November report.[16] The initial recommendations include the development of a universal police report that an identity theft victim can use in presenting their case to creditors and credit reporting agencies. The recommendations also include a roadmap for dealing with government data breaches and a plan for eliminating the unnecessary governmental use of Social Security numbers, because SSNs are the most valuable pieces of consumer information for identity thieves.

B. FTC Outreach

I have mentioned consumer and business education more than once. Time and again we are faced with law enforcement situations that might have been avoided if consumers had been better informed. Education empowers, and nowhere is it more important than in the fight against identity theft. The Commission hosts a toll-free hotline, 1-877-ID THEFT, and a secure online complaint form on its website, www.consumer.gov/idtheft. We receive over 15,000 contacts per week from victims and consumers who want to avoid becoming victims. Callers to the hotline

---

[16] *See* FTC Press Release, *Identity Theft Task Force Announces Interim Recommendations* (Sept. 19, 2006), *available at* http://www.ftc.gov/opa/2006/09/idtheft.htm.

receive counseling from trained personnel (including Spanish-speaking personnel) who, for example, advise victims to obtain their credit reports, request a fraud alert, contact creditors, and file a police report. And just a few months ago, the FTC launched a nationwide ID Theft education program: "AvoID Theft: Deter, Detect, Defend." Materials in the "AvoID Theft: Deter, Detect, Defend" education kit include a victim recovery guide, "Take Charge: Fighting Back Against Identity Theft." The centerpiece of the campaign is a turnkey toolkit – a comprehensive how-to guide on providing consumer education about identity theft. The toolkit, which includes everything from PowerPoint presentations to pamphlets that organizations and others can use in their outreach, will empower consumers to educate each other on identity protection. All materials are available in English and in Spanish. To date, the FTC has distributed more than 22 million publications on identity theft.[17]

C. Legislation

While we are making progress in creating a culture of data security, some believe that the progress would be hastened through new legislation that squarely addresses the recent data breaches and the security issues that they raise. We have spent substantial time working with congressional committees, and we have urged caution in developing a legislative solution.[18]

---

[17] In addition, last September, we announced a partnership with cybersecurity experts, consumer advocates, online marketers and other federal agencies, through which we launched a dynamic consumer education initiative, OnGuardOnline. OnGuardOnline.gov is a new website that provides general information on online safety, interactive educational games that teach consumers how to spot online scams, and specific information on a range of topics, including spyware and phishing. We are delighted at the positive response that the website has received and are encouraging any organization interested in computer security to link to OnGuardOnline.gov.

[18] *See, e.g.*, Prepared Statement of the FTC, *Data Breaches and Identity Theft*, Before the Committee on Commerce, Science, and Transportation of the United States Senate

While it is important that sensitive consumer data be protected, it is also important that legislation not unduly interfere with the free flow of data that allows businesses to offer consumers a wider range of products, services, and payment options; greater access to credit; and faster transactions.

IV. New Security Challenges

A. Pretexting

Another important issue on our agenda – and one that is making headlines everywhere – is the disturbing practice of companies selling consumer telephone records.[19] A number of companies – many of which are online – are peddling cell phone and landline records. According to one website offer, for example, if you provide them with a cell phone number, they will provide you with a list of all outgoing calls in as little as one hour. They will also provide the owner's name, billing address, and home phone number.

Although the acquisition of telephone records may not threaten immediate economic harm, in some ways the consequences could nevertheless be dire. Consider, for example, an abusive ex-husband trying to track down his estranged ex-wife. Or an ex-con trying to track down the law enforcement officer who put him in jail. But for most people – the basic issue is

---

(June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/datasectest.htm;

[19] *See* Prepared Statement of the Federal Trade Commission Before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Affairs, Product Safety, and Insurance (Feb. 8, 2006), *available at* http://www.ftc.gov/os/2006/02/commissiontestimonypretexting060208.pdf; Prepared Statement of the Federal Trade Commission Before the House Committee on Energy and Commerce (Feb. 1, 2006), *available at* http://www.ftc.gov/os/2006/02/commissiontestimonypretexting.pdf.

this: it is an intrusion into their personal privacy. Americans do not want their private call records available to the public.

To combat this threat, the Commission is actively investigating companies that appear to be unlawfully selling phone records or obtaining consumers' phone records by "pretexting," which is the use of false pretenses to obtain sensitive information. In a typical scenario, a pretexter calls the consumer's telephone company, pretends to be the consumer, and asks for his recent phone bill to be faxed to him. This practice not only violates Section 5 of the FTC Act, but it undermines consumers' confidence in the marketplace and in the security of their sensitive data.[20]

This past May, the Commission filed five cases against Web-based operations that obtained and sold consumers' confidential telephone records to third parties. The FTC is seeking a permanent halt to the sale of the phone records, and has asked the courts to order the operators to give up the money they made with their illegal operations.

B. Spyware

Spyware is a computer-related fraud that is causing substantial harm to consumers and to the Internet as a medium of communication and commerce, and the Commission has launched an aggressive law enforcement program to fight spyware. To be sure, spyware presents serious new challenges in detection, apprehension, and enforcement. But through litigation, the FTC has

---

[20] In addition, the practice may violate some state laws that prohibit telephone records pretexting as well as various criminal statutes. *See, e.g.*, 18 U.S.C. § 1343. Similarly, the Gramm-Leach-Bliley Act prohibits pretexting to obtain or attempt to obtain customer information from a financial institution. 15 U.S.C. § 6821.

successfully challenged the distribution of spyware that causes injury to consumers in the online marketplace.

Our law enforcement actions reaffirm three key principles about spyware. First, a consumer's computer belongs to him or her, not to the software distributor. Second, buried disclosures do not work, just as they have never worked in more traditional areas of commerce. And third, if a distributor puts a program on a consumer's computer that the consumer does not want, the consumer must be able to uninstall or disable it.

In the past year, we have initiated seven law enforcement actions relating to spyware.[21] One action charged Odysseus Marketing and its owner with secretly installing spyware on consumers' computers. Our complaint alleges that the defendants deceptively market a program called "Kazanon," which they claim makes users anonymous when using peer-to-peer file-sharing programs. Not only does the program not work as promised – itself a violation of the FTC Act – but it also automatically installs a spyware program on the user's computer that, in turn, automatically installs numerous adware and other programs on behalf of others. The spyware, among other things, replaces or reformats Internet search engine results, generates pop-up ads, and captures and transmits information. Indeed, in discovery, staff found that not only did the spyware degrade the computer's performance, but it also collected personal information

---

[21] *See FTC v. Digital Enterprises, Inc.*, CV 06-4923CAS (C.D. Cal., filed Aug. 9, 2006); *FTC v. Enternet Media, Inc.*, CV05-7777CAS, (C.D. Cal., filed Nov. 1, 2005); *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com, Inc.*, FTC File No. 042 3196 (filed Sept. 12, 2005); *FTC v. Trustsoft, Inc.*, Civ. No. H 05 1905 (S.D. Tex May 31, 2005); *FTC v. MaxTheater, Inc.*, File No. 05-CV-0069 (E.D. Wash. Mar. 8, 2005); *FTC v. Seismic Entertainment, Inc.*, No. 04-377-JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004).

from consumers. Staff obtained preliminary relief to safeguard any information defendants collected.

In another case, brought against Enternet Media and others, the Commission alleged that defendants lured consumers to their websites with the promise of free lyric files, browser upgrades, and ring tones, and then downloaded spyware and adware on consumers' computers. Defendants' software code allegedly tracked consumers' Internet comings and goings, changed home page settings, and displayed pop-up ads on consumers' computers even when consumers' Internet browsers are not activated. Just a few weeks ago, we announced that we have settled this case, with defendants paying $2 million and agreeing to strong injunctive relief that bars them from interfering with a consumer's computer use, including distributing software code that tracks consumers' Internet activity or collects other personal information.[22]

V. Tech-Ade Hearings – Exploring the Future

One of the Commission's most important functions is to study current and emerging marketplace trends to anticipate their significance for consumer protection policy and enforcement. No area of inquiry is more intriguing than the intersection of new technologies and their applications in the global consumer marketplace. Indeed, going forward, issues of data security and privacy will continue to play prominent roles, as consumers and businesses store more and more information on the Internet. This fall, from November 6-9, we will hear from an array of experts from around the world who have been invited to inform us, in public hearings, about what they see as emerging trends, applications, products, services, and issues over the next

---

[22] *See* FTC Press Release, *FTC Closes Door on Spyware Operation* (Sept. 6, 2006), *available at* http://www.ftc.gov/opa/2006/09/enternet.htm.

ten years.[23] We have named these hearings "Protecting Consumers in the Next Tech-Ade", and in the preliminary agenda we recently released on our website, www.ftc.gov, you can get a sense of the exciting issues we will be exploring, ranging from the future of the Internet to new payment systems. What is the impact for consumers of living in an instant information culture? What does user-generated content mean for marketers? Issues of data security and privacy will play significant roles in these discussions.

The hearings will be held at George Washington University's Lisner Auditorium – a venue that provides room for all to attend, engage, and learn along with us. Throughout the fall, we will feature live chat, blogs, and other opportunities on the FTC website to learn about and prepare for the hearings. And if you cannot make it to Lisner, the hearings will be webcast. So please accept our invitation to learn and engage with us on these important issues.

V. Conclusion

Thank you again for the opportunity to speak to you today. I would be glad to spend a few minutes answering questions.

---

[23] Information about the Tech-Ade hearings is available at http://www.ftc.gov/bcp/workshops/techade/index.html.